

Attorney(s) Russ Smith, pro se  
PO Box 1860

Town, State, Zip Code Ocean City, NJ 08226  
 Telephone Number (609) 398-3301  
 Attorney(s) for Plaintiff \_\_\_\_\_

Russ Smith, pro se

\_\_\_\_\_  
 Plaintiff(s)

Vs.

Trusted Universal Standards in Electronic Transactions, Inc  
Microsoft, Inc., Cisco Systems, Inc., Comcast Cable ...  
 Defendant(s)

## Superior Court of New Jersey

Cape May COUNTY  
Chancery DIVISION

Docket No: CPM-C-44 -09

### CIVIL ACTION SUMMONS

*Rec'd 8/6/09*  
*due 9/9 (Thursday?)*

From The State of New Jersey To The Defendant(s) Named Above:

The plaintiff, named above, has filed a lawsuit against you in the Superior Court of New Jersey. The complaint attached to this summons states the basis for this lawsuit. If you dispute this complaint, you or your attorney must file a written answer or motion and proof of service with the deputy clerk of the Superior Court in the county listed above within 35 days from the date you received this summons, not counting the date you received it. (The address of each deputy clerk of the Superior Court is provided.) If the complaint is one in foreclosure, then you must file your written answer or motion and proof of service with the Clerk of the Superior Court, Hughes Justice Complex, P.O. Box 971, Trenton, NJ 08625-0971. A filing fee payable to the Treasurer, State of New Jersey and a completed Case Information Statement (available from the deputy clerk of the Superior Court) must accompany your answer or motion when it is filed. You must also send a copy of your answer or motion to plaintiff's attorney whose name and address appear above, or to plaintiff, if no attorney is named above. A telephone call will not protect your rights; you must file and serve a written answer or motion (with fee of \$135 and completed Case Information Statement) if you want the court to hear your defense.

If you do not file and serve a written answer or motion within 35 days, the court may enter a judgment against you for the relief plaintiff demands, plus interest and costs of suit. If judgment is entered against you, the Sheriff may seize your money, wages or property to pay all or part of the judgment.

If you cannot afford an attorney, you may call the Legal Services office in the county where you live. A list of these offices is provided. If you do not have an attorney and are not eligible for free legal assistance, you may obtain a referral to an attorney by calling one of the Lawyer Referral Services. A list of these numbers is also provided.

Dated: 7/29/09

for Jennifer M. Perez  
 Jennifer M. Perez,  
 Acting Clerk of the Superior Court

Name of Defendant to Be Served: Comcast Cable Communications, LLC

Address of Defendant to Be Served: 341 West Ave. Ocean City, NJ 08226

NOTE: The Case Information Statement is available at <http://www.njcourtsonline.com>



# CIVIL CASE INFORMATION STATEMENT (CIS)

Use for initial Law Division  
Civil Part pleadings (not motions) under Rule 4:5-1  
Pleading will be rejected for filing, under Rule 1:5-6(c),  
if information above the black bar is not completed or  
if attorney's signature is not affixed.

PAYMENT TYPE: CK CG CA

CHG/CK NO.

AMOUNT:

OVERPAYMENT:

BATCH NUMBER:

1. ATTORNEY/PRO SE NAME Russ Smith, pro se		2. TELEPHONE NUMBER (609) 398-3301		3. COUNTY OF VENUE Cape May	
4. FIRM NAME (if applicable)				5. DOCKET NUMBER (When available)	
6. OFFICE ADDRESS PO Box 1860 Ocean City, NJ 08226 <i>131 Wesley Ave Ocean City, NJ 08226</i>				7. DOCUMENT TYPE Complaint	
9. NAME OF PARTY (e.g., John Doe, Plaintiff) Russ Smith, Plaintiff				8. JURY DEMAND <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO	
10. CAPTION Russ Smith, pro se v. Trusted Universal Standards in Electronic Transactions, Inc. (d/b/a, TRUSTe, Inc.), Microsoft, Inc., Cisco Systems, Inc., and Comcast Cable Communications, LLC					
11. CASE TYPE NUMBER (See reverse side for listing) 599		12. IS THIS A PROFESSIONAL MALPRACTICE CASE? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO IF YOU HAVE CHECKED "YES," SEE N.J.S.A. 2A:53A-27 AND APPLICABLE CASE LAW REGARDING YOUR OBLIGATION TO FILE AN AFFIDAVIT OF MERIT.			
13. RELATED CASES PENDING? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		14. IF YES, LIST DOCKET NUMBERS			
15. DO YOU ANTICIPATE ADDING ANY PARTIES (arising out of same transaction or occurrence)? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		16. NAME OF DEFENDANT'S PRIMARY INSURANCE COMPANY, IF KNOWN <input type="checkbox"/> NONE <input checked="" type="checkbox"/> UNKNOWN			

THE INFORMATION PROVIDED ON THIS FORM CANNOT BE INTRODUCED INTO EVIDENCE.

CASE CHARACTERISTICS FOR PURPOSES OF DETERMINING IF CASE IS APPROPRIATE FOR MEDIATION					
17. A. DO PARTIES HAVE A CURRENT, PAST OR RECURRENT RELATIONSHIP? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO		IF YES, IS THAT RELATIONSHIP <input type="checkbox"/> EMPLOYER-EMPLOYEE <input type="checkbox"/> FRIEND/NEIGHBOR <input type="checkbox"/> OTHER (explain) <input checked="" type="checkbox"/> FAMILIAL <input checked="" type="checkbox"/> BUSINESS			
18. B. DOES THE STATUTE GOVERNING THIS CASE PROVIDE FOR PAYMENT OF FEES BY THE LOSING PARTY? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO					
19. USE THIS SPACE TO ALERT THE COURT TO ANY SPECIAL CASE CHARACTERISTICS THAT MAY WARRANT INDIVIDUAL MANAGEMENT OR ACCELERATED DISPOSITION:  Case involves NJ Consumer Fraud Act, contractual obligations, and defamation. I chose 599 as the case type because I believe, at this time, that 300 days discovery will be sufficient for this matter.					
20. DO YOU OR YOUR CLIENT NEED ANY DISABILITY ACCOMMODATIONS? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		IF YES, PLEASE IDENTIFY THE REQUESTED ACCOMMODATION:			
21. WILL AN INTERPRETER BE NEEDED? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO		IF YES, FOR WHAT LANGUAGE:			
22. ATTORNEY SIGNATURE <i>Russ Smith</i> <i>7/29/09</i>					

Russ Smith, *pro se*

Plaintiff,

v.

Trusted Universal Standards in

Electronic Transactions, Inc. (d/b/a,

TRUSTe, Inc.),

Microsoft, Inc.,

Cisco Systems, Inc., and

Comcast Cable Communications, LLC

Defendants

: SUPERIOR COURT OF NEW  
: JERSEY  
: CAPE MAY COUNTY:  
: CHANCERY DIVISION  
: GENERAL EQUITY

: CIVIL ACTION

: COMPLAINT

: Docket No.: CPM-C- 44 -09

---

1. Plaintiff Russ Smith is a resident of Ocean City, NJ.

**Summary**

2. Defendants have, for many years, promoted a scenario of "self regulation" in the area of privacy and the collection of personal information.

3. Plaintiff asserts that

- a. Defendants Microsoft, Cisco, and Comcast have developed Internet "profiles" of Plaintiff by intercepting Internet communications and other means,
- b. Defendants Microsoft, Cisco and Comcast have posted false and misleading privacy policies and other false and misleading policies and representations,
- c. Defendant TRUSTe has conspired with Microsoft, Cisco and Comcast to promote web site privacy policies and other policies which are false, contradictory, and/or misleading,

- d. Defendant TRUSTe has operated a privacy policy verification service where they charged seal holders a fee to promote a privacy policy verification service which is fraudulent and meant to dupe Internet users and regulatory officials, and
  - e. Defendant TRUSTe has operated a fraudulent dispute resolution service, and
  - f. Microsoft and Cisco have defamed Plaintiff by distributing false and misleading reports to third parties causing Plaintiff's Internet mail communications to be repeatedly blocked.
  - g. Microsoft, Cisco, and Comcast failed to honor their privacy policies that have provisions that would allow Plaintiff to review the profiles, Personally Identifiable Information (PII), and other information they collected about Plaintiff, such as the information that lead to the defamatory reports that caused Plaintiff's Internet mail communications to be repeatedly blocked.
4. Plaintiff seeks relief under the New Jersey Consumer Fraud Act N.J.S.A 56:8-2 et seq. to:
- a. Enforce the posted privacy policies and various contracts, agreements, and web site representations of Defendants,
  - b. Prohibit Defendants from posting false and misleading privacy and other policies and representations on their respective web sites,
  - c. Require Defendants Cisco, Microsoft, and Comcast to allow Plaintiff to review account, other information collected about him, Personally Identifiable Information (PII) information, and reports to third parties so Plaintiff may review and correct any incorrect or false information.

5. Plaintiff seeks to enforce various contracts and agreements as a result of Plaintiff's subscription to Comcast Internet services and representations and contracts displayed at various web sites operated by Defendants.
6. Plaintiff seeks relief to stop Comcast, Microsoft, and Cisco from intercepting Plaintiff's Internet communications pursuant to the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1], Federal Wiretap Law [18 USC § 2510 et seq.], and/or The Pen Register Act [18 USC § 3121 et seq.].
7. Plaintiff seeks relief to prohibit Defendants from defaming Plaintiff by transmitting information collected as a result of eavesdropping on Plaintiff's Internet communications, the development of erroneous profiles, and/or using incorrect information collected from third parties.

**Defendant TRUSTe**

8. Defendant Trusted Universal Standards in Electronic Transactions, Inc. (d/b/a, TRUSTe, Inc.) ("TRUSTe") is a not-for-profit corporation organized under the laws of California operating at 55 2nd Street, 2nd Floor San Francisco, CA 94105, is classified as a Section 501(c)(6) entity under the Internal Revenue Code, and does business in New Jersey.
  - a. The purpose of Section 501(c)(6) entities is to promote the common business interest and not to engage in a regular business of a kind ordinarily carried on for profit. Its activities are directed to the improvement of business conditions of one or more lines of business rather than the performance of particular services for individual persons.

b. TRUSTe purports its mission to *"Build Trust Through Privacy"* and *"helps consumers and businesses identify trustworthy online organizations through its Web Privacy Seal ... resolves thousands of individual privacy disputes every year ...[by] promoting privacy policy disclosure, informed user consent, and consumer education ...[and] acts as an independent, unbiased trust entity."*

c. Defendant TRUSTe claims:

*"The TRUSTe privacy program – based on a branded online seal, the TRUSTe "trustmark" – bridges the gap between users' concerns over privacy and Web sites' needs for self-regulated information disclosure standards."*

9. TRUSTe is funded by collecting fees and sponsorships from the companies, such as Defendants Comcast and Microsoft, that subscribe to the privacy seal verification program.

10. TRUSTe operates a web site at [www.truste.org](http://www.truste.org) and provides a "watchdog" complaint service where Internet users can verify web site privacy policies and file complaints about companies that display the TRUSTe verification seal on their web site privacy policies.

11. The TRUSTe web site says:

- a. *TRUSTe also provides ... an easy-to-use privacy dispute resolution service free to consumers who encounter problems with their personal information on TRUSTe-approved sites.*
- b. *The TRUSTe Watchdog Dispute Resolution program provides free online third-party privacy dispute resolution to anyone who files an eligible complaint about a TRUSTe Licensee.*
- c. *The Watchdog Dispute Resolution program lets TRUSTe mediate between the individual complainant and the Licensee. The individual's right to legal recourse is not affected. While TRUSTe's*

*final determination is not binding on the individual, the Licensee must comply with TRUSTe's final determination or face removal from the TRUSTe program, possible publication of that removal, and/or referral to an appropriate law-enforcement body.*

**Defendant Comcast**

12. Defendant Comcast Cable Communications, LLC ("Comcast") has a business office at 341 West Ave, Ocean City, NJ and offers Broadband Internet services to Plaintiff and many other citizens of New Jersey.

13. Plaintiff is a customer of Comcast and subscribes to Broadband Internet Services.

14. On or about May 16, 2004 Plaintiff notified Comcast of the choice to "opt-out" of the binding arbitration clause added to the Comcast User Agreement.

15. The Comcast Privacy Policy at <http://www.comcast.net/privacy/> is endorsed by the TRUSTe privacy seal.

16. The Comcast "2009 Comcast Customer Privacy Notice" found at <http://www.comcast.com/customerprivacy/> is part of the policy endorsed by the TRUSTe privacy seal.

17. The Comcast "2009 Comcast Customer Privacy Notice" states:

- a. *"How can I see my personally identifiable information [PII] or CPNI and correct it, if necessary? You may examine and correct, if necessary, the personally identifiable information regarding you that is collected and maintained by Comcast in our regular business records."*

18. Defendant's Network Management FAQ states:

- a. *Will the technique target P2P or other applications, or make decisions about the content of my traffic?*

*No. The new technique is "protocol-agnostic," which means that the system does not manage congestion based on the applications being used by customers. It is content neutral, so it does not depend on the type of content that is generating traffic congestion. Said another way,*



*customer traffic is congestion-managed not based on their applications, but based on current network conditions and recent bytes transferred by users.*

**Defendant Microsoft**

19. Defendant Microsoft, Inc. ("Microsoft") is registered with the State on New Jersey under business ID 0100568573 with a registered agent at 830 Bear Tavern Rd., West Trenton, NJ 08628.
20. Microsoft operates The "Frontbridge" services which compiles information about Internet mail servers by intercepting Internet e-mail traffic and creates IP address "blacklists/blocklists". These "blacklists" are then distributed to third parties or used by those using Microsoft services for the purpose of blocking e-mail communications of the IP addresses on the blacklists.
21. The Microsoft Frontbridge services are described at the web site <http://www.FrontBridge.com>. Users typing in [www.frontbridge.com](http://www.frontbridge.com) are redirected to the web page <http://www.microsoft.com/online/exchange-hosted-services.mspx>. This web page contains a link to a "privacy statement" at <http://privacy.microsoft.com/en-us/default.mspx> which is endorsed by the TRUSTe privacy seal verification program.
22. Microsoft's privacy policy at <http://privacy.microsoft.com/en-us/fullnotice.mspx#accessing> states:
  - a. *Accessing Your Personal Information ... You may have the ability to view or edit your personal information online ... Some Microsoft sites or services may collect personal information that is not accessible via the links above. However, in such cases, you may be able to access that information through alternative means of access described by the service. Or you can write us by using our Web form, and we will contact you within 30 days regarding your request.*



**Defendant CISCO**

23. Defendant Cisco Systems, Inc. ("Cisco") is registered with the State on New Jersey under business ID 0100437778 with a registered agent at 830 Bear Tavern Rd., West Trenton, NJ 08628.
24. Defendant Cisco operates a web site at [www.cisco.com](http://www.cisco.com). Cisco also a service called IronPort and operates web sites [www.ironport.com](http://www.ironport.com) and [www.senderbase.org](http://www.senderbase.org) as part of this service.
25. Cisco collects data on more than 25 percent of the world's email traffic and claims their service claims the service can be used *"like a credit reporting service for email, providing comprehensive data that ISPs and companies can use to differentiate legitimate senders from spammers and other attackers and giving email administrators visibility into who is sending them email."* Cisco develops a "reputation" score for Internet IP addresses and distributes this "reputation" to third parties.
26. The Cisco privacy policy at <http://cisco.com/web/siteassets/legal/privacy.html> states:

*Collection of your personal information[:] We will always tell you before we collect any Personal Information and inform you of the purpose of the collection. "Personal Information" is any information that can be used to identify an individual, and may include, but is not limited to, name, email address, postal or other physical address, credit or debit card number, title, occupation, and other information required to provide a service, deliver a product, or carry out a transaction you have requested. ... We need your help in keeping the Personal Information you have shared with us accurate and up to date. Please notify us of any changes to your Personal Information.*

**Microsoft "Blacklisting" Plaintiff**

27. On or about July 3, 2008 Microsoft included the IP address of Plaintiff's e-mail server in a "blacklist" distributed to third parties which resulted in the blocking of Plaintiff's e-mail communications.

28. Microsoft eavesdrops on Internet communications in violation of the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A. 2A:156A-1], Federal Wiretap Law [18 USC § 2510 et seq.], and/or The Pen Register Act [18 USC § 3121 et seq.] in order to collect information to place Internet IP addresses on various blacklists.

29. On or about July 7, 2008 Microsoft communicated to Plaintiff:

*"...Unfortunately we do not retain examples of the type of spam as evidence however we do keep logs of the sender/recipient information and the message ID and will be provided when the information is available. Unfortunately it is taking longer for us to provide this information as we are attempting to determine when this IP was first listed on our blacklist. Our blacklisting system will not list an IP address unless there is a large volume of spam being captured for a domain."*

30. Microsoft did not provide Plaintiff any information that led to the blacklist placement or any evidence of "spam" or associated logs.

31. On or about September 23, 2008 Microsoft again placed Plaintiff on a blacklist that resulted in e-mail communications of Plaintiff being blocked and did not provide Plaintiff any information that led to the blacklist placement.

32. Plaintiff filed TRUSTe Watchdog Complaint #43304 against Microsoft.

33. TRUSTe responded by claiming:

- a. *"...We have determined that the matter does not fall within the scope of our program. We are therefore unable to address your complaint. The link to the main Microsoft privacy policy is for the web site's marketing program. Users who sign up with the Frontbridge service are offered a different privacy policy (this works the same way for the*

*Microsoft Office stand-alone program versus Office Online). TRUSTe does not certify Frontbridge operations and we have no jurisdiction over this matter..."*

- b. Plaintiff notified TRUSTe that
  - i. users blacklisted were directed to www.frontbridge.com which displays a link to the TRUSTe-endorsed privacy policy seal,
  - ii. those on the blacklist did not sign up for any FrontBridge service and were not bound by any contract other than what was displayed at the web site and that Plaintiff did not "sign up" for the Frontbridge service.
- c. TRUSTe failed to prove a reasonable response that addressed issues or take reasonable action to ensure Microsoft complied with the TRUSTe program requirements.

34. Microsoft paid TRUSTe to have a seat on the TRUSTe Advisory Council.

**Comcast Blocking E-mail Communications of Plaintiff**

35. Comcast eavesdrops on Internet communications of Plaintiff in violation of the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1], Federal Wiretap Law [18 USC § 2510 et seq.], and/or The Pen Register Act [18 USC § 3121 et seq.].

36. Comcast permits third parties, including Cisco, to eavesdrop on Internet communications of Plaintiff in violation of the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1], Federal Wiretap Law [18 USC § 2510 et seq.], and/or The Pen Register Act [18 USC § 3121 et seq.].

37. Comcast maintains contradictory policies posted at its web sites that claim:

- a. *"customer traffic is congestion-managed not based on their applications, but based on current network conditions and recent bytes transferred by users" [Network Management Policy] and*
- b. *We will not read your outgoing or incoming e-mail... We also monitor the performance of our Service and your Service connection in order to manage, maintain, and improve the Service and your connection to it. We (or our third party providers) use tools to help prevent and block "spam" e-mails, viruses, spyware, and other harmful or unwanted communications and programs on the Service. These tools may automatically scan your e-mails ... and other files and communications in order to help us protect you and the Service against these harmful or unwanted communications and programs. However, these tools do not collect or disclose personally identifiable information about you..." [Privacy Policy effective January 1, 2009].*

38. On or about March 9, 2009 Comcast blocked all outbound e-mail communications from Plaintiff's Internet account.

39. Upon calling Comcast Plaintiff was told Comcast detected "spam e-mail" coming from Plaintiff's account. Plaintiff asked Comcast to provide the evidence so Plaintiff could see what is wrong and fix it. Comcast refused and said the information was "proprietary." Plaintiff pointed to the Comcast privacy policy that states customers can review the information maintained in the account. Comcast told me it didn't matter what the privacy policy said, they said the information was proprietary and Plaintiff wasn't getting it. Comcast told Plaintiff they would unblock the e-mail port this one time. Comcast would not tell Plaintiff why it was blocked but if similar activity was detected Plaintiff be permanently blocked from sending e-mail unless Plaintiff paid for a higher level of service. Plaintiff was told he would not have to worry about any e-mail blocking if Plaintiff subscribed to a higher level of service.

40. Comcast later claimed to Plaintiff in a letter dated April 6, 2009 that the blocking was due to a report from a third party, IronPort, owned by Cisco and a so-called IP address "reputation." Cisco later claimed another third party

outside the United States, Spamhaus, actually made the report. Spamhaus web site claimed the "poor reputation" was based on spam originating from all of the Comcast networks and that all Comcast network addresses were given a poor reputation and that no specific "spam e-mail" was detected from Plaintiff's Comcast account.

41. Such an explanation is absurd since this would result in all Comcast IP addresses being given the same poor reputation by Cisco and, therefore, Comcast would block all e-mail from all of its customers.
42. On or about April 16, 2009 Comcast again blocked all outbound communications of Plaintiff and did not provide an explanation.
43. Plaintiff filed a TRUSTe Watchdog complaint number 48106 and the response to Plaintiff stated:
  - a. *"The Web site has cooperated with TRUSTe and has provided the information they used to base their service decision. The further issues you raise are outside the scope of TRUSTe's privacy program."*
44. Plaintiff complained to TRUSTe that the responses received from Comcast and their posted policies were contradictory and could not fulfill a legitimate compliance and audit procedure. TRUSTe failed to prove a reasonable response that addressed issues or take reasonable action to ensure Comcast complied with the TRUSTe program requirements.
45. Comcast has subsequently blocked access to Plaintiff of all his account information and Plaintiff.
46. Comcast is violating 47 C.F.R. § 76.1716 by refusing to allow Plaintiff access to his account information.

**Cisco Fraudulently Operating E-mail "Credit" Reporting Service**

47. Cisco uses its position in the sale and distribution of Internet devices, such as routers and switches, to install Internet monitoring devices in thousands of networks around the world.
48. Cisco eavesdrops on Internet communications in violation of the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1], Federal Wiretap Law [18 USC § 2510 et seq.], and/or The Pen Register Act [18 USC § 3121 et seq.] in order to collect information to give IP addresses "reputation" scores.
49. Cisco claims to operate a "Credit" Reporting Service for e-mail and develops a "reputation" score for Internet IP addresses and reports and publishes this information to third parties.
50. Plaintiff made several requests to Cisco to obtain the information they collected to produce a "reputation" score about Plaintiff's Internet connection IP address.
51. Cisco pointed Plaintiff to a "reputation" web page that claimed the "reputation" score was actually taken from another third party in the United Kingdom, Spamhaus. Spamhaus web site claimed the "poor reputation" was based on spam originating from all of the Comcast networks and that all Comcast network addresses were given a poor reputation and that no specific "spam e-mail" was detected from Plaintiff's Comcast account.
52. Such an explanation by Cisco is absurd since this would result in all Comcast IP addresses being given the same poor reputation by Cisco and, therefore, Comcast would block all e-mail from all of its customers.

**Counts - TRUSTe**

- 53. TRUSTe made false and misleading representations at its web site in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual requirements to offer a dispute resolution service by:**
- 54. Count 1:** failing to provide a reasonable resolution to complaint filed by Plaintiff against Microsoft,
- 55. Count 2:** failing to remove Microsoft from the TRUSTe program after being aware of non-compliance with the program requirements,
- 56. Count 3:** failing to take reasonable action after being aware Microsoft posted fraudulent or misleading privacy policy and other representations at their web sites,
- 57. Count 4:** failing to take reasonable action after being aware Microsoft did not allow Plaintiff to have access to the PII Microsoft collected about Plaintiff,
- 58. Count 5:** failing to take reasonable action after being aware Microsoft did not allow Plaintiff to correct the PII Microsoft has collected about Plaintiff,
- 59. Count 6:** failing to provide a reasonable resolution to complaint filed by Plaintiff against Comcast,
- 60. Count 7:** failing to remove Comcast from the TRUSTe program after being aware of non-compliance with the program requirements,
- 61. Count 8:** failing to take reasonable action after being aware Comcast posted fraudulent or misleading privacy policy and other representations at their web sites,
- 62. Count 9:** failing to take reasonable action after being aware Comcast did not allow Plaintiff to have access to the PII and other information Comcast collected about Plaintiff, and



**63. Count 10:** failing to take reasonable action after being aware Comcast did not allow Plaintiff to correct the PII Comcast has collected about Plaintiff.

**Counts - Comcast**

**64. Count 11:** Comcast violated the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**65. Count 12:** Comcast violated the Federal Wiretap Law [18 USC § 2510 et seq.] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**66. Count 13:** Comcast violated the Pen Register Act [18 USC § 3121 et seq.] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**67. Comcast** made false and misleading representations in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual agreements with Plaintiff by:

**68. Count 14:** not providing Plaintiff access the PII Comcast compiled about Plaintiff,

**69. Count 15:** not providing Plaintiff access the PII Comcast compiled about Plaintiff,

**70. Count 16:** by not allowing Plaintiff to correct the PII Comcast has collected about Plaintiff,

**71. Count 17:** providing a false and/or misleading explanation of why Plaintiff's e-mail communications were blocked,

14+15  
same

**72. Count 18:** monitoring and blocking specific protocols and services, such as e-mail, while making the representation that monitoring and blocking is "protocol agnostic," and

**73. Count 19:** by posting various policies at its web site which are inconstant about how Internet communications are monitored and/or blocked.

**74. Count 20:** Comcast has violated its agreement with the City of Ocean City, NJ by not allowing Plaintiff access the PII they compiled about Plaintiff.

**75. Count 21:** Comcast has violated the Cable Communications Policy Act of 1984 by not allowing Plaintiff access his account information.

**Counts - Microsoft**

**76. Microsoft** made false and misleading representations in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual agreements with Plaintiff by:

**77. Count 22:** claiming the Microsoft Privacy Policy does not apply to their Frontbridge Service by:

- a. redirecting Internet users who typed in [www.FrontBridge.com](http://www.FrontBridge.com) to a web page at Microsoft.com, and then
- b. claiming that the Microsoft privacy policy does not apply to the Frontbridge service and/or [www.FrontBridge.com](http://www.FrontBridge.com).

**78. Count 23:** by not providing Plaintiff access the PII Microsoft compiled about Plaintiff.

**79. Count 24:** by not allowing Plaintiff to correct the PII Microsoft has collected about Plaintiff, and

**80. Count 25:** by not following through with a promise to Plaintiff to send PII and/or e-mail logs Microsoft has collected about Plaintiff.

**81. Count 26:** Microsoft defamed Plaintiff by placing his IP address on blacklists/blocklists for e-mail communications without allowing Plaintiff to review and correct, if necessary, the information that led to these blacklist/blocklist listings.

**Counts - Cisco**

**82. Cisco** made false and misleading representations in violation of the New Jersey Consumer Fraud Act and/or has failed to comply with its contractual agreements with Plaintiff by:

**83. Count 27:** not providing Plaintiff access the PII Cisco compiled about Plaintiff,

**84. Count 28:** not allowing Plaintiff to correct the PII Cisco collected about Plaintiff,

**85. Count 29:** not following through with a promise to Plaintiff to send PII Cisco has collected about Plaintiff,

**86. Count 30:** claiming Spamhaus was responsible for the poor reputation score of Plaintiff's IP address, and

**87. Count 31:** falsely advertising their Ironport service as being like a credit reporting service for e-mail.

**88. Count 32:** Cisco violated the New Jersey Wiretapping and Electronic Surveillance Control Act [N.J.S.A 2A:156A-1] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**89. Count 33:** Cisco violated the Federal Wiretap Law [18 USC § 2510 et seq.] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

**90. Count 34:** Cisco violated the Pen Register Act [18 USC § 3121 et seq.] by monitoring Plaintiff's Internet communications and/or allowing third parties to do so.

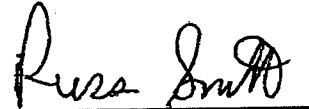
**91. Count 35:** Cisco defamed Plaintiff by giving a reputation score for e-mail communications to plaintiff's IP address without allowing Plaintiff to review and correct, if necessary, the information that led to the reputation score.

**Relief Sought**

**92.** The following relief is sought:

- a. Prohibit Microsoft, Comcast and Cisco from eavesdropping on Internet communications of the citizens of New Jersey, and
- b. Prohibit Comcast displaying or distributing false or misleading portions of the Privacy Policy, Customer Privacy Notice, Acceptable Use Policy for High-Speed Internet Services, Network Management Policy, Network Management FAQ, Spam Policy and other related information to the citizens of New Jersey, and
- c. Prohibit Microsoft from displaying or distributing false or misleading portions of the Privacy Statement and other related information to the citizens of New Jersey, and
- d. Prohibit Cisco from displaying or distributing false or misleading portions of the Privacy Statement and other related information to the citizens of New Jersey, and
- e. Prohibit TRUSTe from conducting a false or misleading dispute resolutions services to the citizens of New Jersey, and
- f. Prohibit TRUSTe from endorsing any privacy policies displayed to citizens of New Jersey, and

- g. Require Microsoft, Comcast and Cisco to provide Plaintiff with all information collected about Plaintiff's Internet communications or any associated data or any PII and allow Plaintiff to correct any erroneous information, and
- h. Prohibit Microsoft, Comcast and Cisco from distributing any defamatory information about Plaintiff to any third party,
- i. Costs of this action, and
- j. Any other action the Court deems just and equitable.



Russ Smith, *pro se*

July 29, 2009

### **CERTIFICATION OF NO OTHER ACTIONS**

I certify that the dispute about which I am suing is not the subject of any other action pending in any other court or a pending arbitration proceeding to the best of my knowledge and belief. Also, to the best of my knowledge and belief no other action or arbitration proceeding is contemplated. Further, other than the parties set forth in this complaint, I know of no other parties that should be made a part of this lawsuit. In addition, I recognize my continuing obligation to file and serve on all parties and the court an amended certification if there is a change in the facts stated in this original certification.

Dated: 7/29/09 Signature: Russ Smith